

Doodler Gebruikersvoorwaarden

Versie 3.5 – 17 november 2025

Geldigheid: Pilotfase 1 (November 2025 - Februari 2026)

Contactpersoon: Mayra Kapteijn (mayra@doodler.app)

1. Definities

Het Verbond B.V. ("Doodler") – de rechtspersoon die Doodler ontwikkelt en exploiteert, gevestigd te Amsterdam, en optreedt als verwerker in de zin van de AVG.

Gebruiker – de jeugd-GGZ-instelling die Doodler inzet binnen de pilot en optreedt als verwerkingsverantwoordelijke in de zin van de AVG.

Subverwerkers –

- Glanos GmbH (Duitsland) levert een webomgeving voor automatische pseudonimisering van tekstdata. Glanos beschikt over een ISAE 3402 type 2 assurance rapport voor informatiebeveiliging en maakt gebruik van Europese datacenters van onder meer Hetzner en OVHcloud die ISO 27001 gecertificeerd zijn en technische en organisatorische maatregelen toepassen volgens artikel 32 AVG.
- Microsoft Ireland Operations Ltd. levert het Azure cloudplatform en de Azure OpenAI diensten voor verwerking binnen de EU regio. Azure is ISO 27001 gecertificeerd en biedt een NEN 7510 dekkingsrapport op platformniveau.

Gepseudonimiseerde gegevens – tekstdata waarvan persoonsherleidbare informatie is verwijderd of vervangen door middel van pseudonimisering via Glanos, uitgevoerd door de Gebruiker vóór invoer in Doodler.

2. Doel en aard van de dienstverlening

Doodler ondersteunt behandelaren door tekst uit het EPD om te zetten naar visuele praatplaten voor gebruik in advies- en behandelgesprekken.

Doodler is geen medisch hulpmiddel in de zin van de MDR en levert geen diagnostische

of therapeutische beslissingsondersteuning, en valt daardoor niet onder de reikwijdte van de Europese Verordening Medische Hulpmiddelen (EU) 2017/745.

De pilot heeft een experimenteel karakter:

- doel is het valideren van de bruikbaarheid en veiligheid van Doodler;
 - er worden geen structurele verplichtingen aangegaan;
 - alle verwerking vindt plaats onder toezicht en verantwoordelijkheid van gebruiker.
-

3. Rollen en gegevensverwerking

3.1 Verwerkingsverantwoordelijkheid

De Gebruiker is verwerkingsverantwoordelijke; Het Verbond B.V. is verwerker.

De verwerking vindt uitsluitend plaats ten behoeve van de pilot binnen de overeengekomen doelen en grenzen.

Het Verbond B.V. houdt een intern register van verwerkingen bij dat de aard, doelen en subverwerkers beschrijft en stelt dit op verzoek beschikbaar aan de Gebruiker.

3.2 Pseudonimisering en gebruik van Glanos

De pseudonimisering van tekstdata wordt uitgevoerd door de Gebruiker binnen de door Het Verbond B.V. beschikbaar gestelde Glanos webomgeving.

De Gebruiker logt zelfstandig in bij Glanos, uploadt de tekst inclusief persoonsgegevens en downloadt vervolgens de door Glanos gepseudonimiseerde versie. Deze gepseudonimiseerde tekst wordt daarna door de Gebruiker geüpload in Doodler.

Glanos verwerkt tekstdata tijdelijk binnen Europese datacenters. De originele tekst wordt na afronding van de verwerking volgens het Glanos verwijderbeleid automatisch verwijderd en in ieder geval binnen een korte, vooraf vastgelegde termijn.

De Gebruiker blijft als verwerkingsverantwoordelijke verantwoordelijk voor de beoordeling of de gepseudonimiseerde gegevens voor derden redelijkerwijs niet herleidbaar zijn. Het Verbond B.V. is uitsluitend verantwoordelijk voor de werking en beveiliging van het door

haar geleverde pseudonimiseringsmiddel. Restinformatie die voortkomt uit de ingevoerde tekst valt onder verantwoordelijkheid van de Gebruiker.

Subverwerkerstatus Glanos

Glanos treedt in dit kader op als subverwerker van Het Verbond B.V., uitsluitend voor zover deze dienst door Het Verbond B.V. aan de Gebruiker wordt gefaciliteerd. De verwerking door Glanos vindt volledig plaats binnen de Europese Economische Ruimte.

Nieuwe subverwerkers

Eventuele nieuwe subverwerkers worden uitsluitend na voorafgaande schriftelijke kennisgeving aan de Gebruiker ingeschakeld.

3.3 Verwerking binnen Doodler

De door de Gebruiker aangeleverde gepseudonimiseerde gegevens worden verwerkt binnen Microsoft Azure in de regio Noord-West Europa.

Binnen Azure OpenAI is in deze pilot een beleid van nulretentie geconfigureerd. Gegevens worden uitsluitend tijdelijk gebruikt om output te genereren en worden daarna direct automatisch verwijderd. De gegevens worden niet opgeslagen voor modeltraining of andere doeleinden.

Omdat Doodler geen toegang heeft tot de oorspronkelijke gegevens en geen hulpmiddelen bezit waarmee identificatie mogelijk is, kwalificeren de ontvangen gegevens voor Doodler zelf niet als persoonsgegevens in de zin van de AVG. Voor de Gebruiker blijven de oorspronkelijke gegevens onder de AVG vallen, aangezien de Gebruiker over de identificerende broninformatie beschikt.

3.4 Informatieplicht en rechten van betrokkenen

De Gebruiker blijft verantwoordelijk voor het informeren van cliënten over het gebruik van Doodler, de wijze van pseudonimisering en de betrokken partijen (waaronder Glanos en Microsoft).

Het Verbond B.V.:

- ondersteunt desgewenst bij DPIA's en privacydocumentatie;
- verleent volledige medewerking aan de uitvoering van rechten van betrokkenen;
- draagt ervoor zorg dat een ontvangen verzoek van een betrokkene binnen 2 werkdagen wordt doorgestuurd naar de Gebruiker.

3.5 Werkproces en handleiding

De Gebruiker draagt zorg dat behandelaren Doodler uitsluitend gebruiken volgens de vastgestelde werkwijze waarbij alle tekst vooraf wordt gepseudonimiseerd via Glanos, voordat verwerking binnen Doodler plaatsvindt.

Het Verbond B.V. stelt hiervoor een korte **officiële gebruikershandleiding** beschikbaar die tijdens de aftrap van de pilot wordt toegelicht. Deze handleiding beschrijft stap-voor-stap:

- hoe tekst via Glanos wordt gepseudonimiseerd;
- hoe de geanonimiseerde output in Doodler wordt ingevoerd;
- en welke privacyrichtlijnen behandelaren dienen te volgen.

De Gebruiker zorgt ervoor dat behandelaren deze werkwijze naleven.

4. Beveiliging

Het Verbond B.V. verwerkt zelf geen ruwe cliëntdata. Alle verwerking van gepseudonimiseerde gegevens vindt plaats binnen de omgevingen van de subverwerkers en binnen de eigen Azure omgeving van Doodler.

Microsoft Azure is ISO 27001 gecertificeerd. Glanos beschikt over een ISAE 3402 type 2 assurance rapport. Het Verbond B.V. en de Gebruiker werken volgens de normen en uitgangspunten van NEN 7510 voor informatiebeveiliging in de zorg, zonder dat dit een formele certificeringsclaim van Het Verbond B.V. inhoudt.

Binnen deze kaders wordt voorzien in:

- encryptie tijdens transport en verwerking
- toegangsbeheer op basis van need to know
- logging, monitoring en auditing
- automatische verwijdering van tijdelijke gegevens na verwerking binnen Azure OpenAI en binnen Glanos

Het Verbond B.V. is verantwoordelijk voor de beveiliging van de applicatielaag en past privacy by design en privacy by default toe in alle onderdelen van de software. Het Verbond B.V. voert een maandelijkse vulnerability scan uit over de open source componenten in de broncode en stuurt hiervan desgevraagd een overzicht naar Gebruikers.

Het Verbond B.V. hanteert een intern beveiligingsbeleid in lijn met ISO 27001 en NEN 7510 en past de principes van NEN 7512 (veilige netwerkverbindingen) en NEN 7513 (logging en herleidbaarheid) toe, voor zover redelijk en relevant binnen de pilotfase waarin geen herleidbare persoonsgegevens door Doodler worden opgeslagen of verwerkt.

Concreet betekent dit dat Doodler draait binnen een eigen Microsoft Azure omgeving in de EU regio, waarbij alle gegevens tijdens transport via TLS en in opslag standaard worden versleuteld volgens de standaarden van Microsoft. Toegang tot deze omgeving verloopt via Azure Active Directory met verplichte multifactorauthenticatie. Alleen geautoriseerde medewerkers van Het Verbond B.V. en geautoriseerde medewerkers van de subverwerkers Glanos en Microsoft hebben toegang, binnen de in de verwerkersovereenkomsten vastgelegde reikwijdte.

Netwerkverbindingen zijn ingericht volgens de principes van NEN 7512 door uitsluitend versleutelde verbindingen toe te staan, beheer uitsluitend via beveiligde beheerkanalen mogelijk te maken en geen databronnen rechtstreeks vanaf het internet benaderbaar te maken.

Logging en herleidbaarheid zijn ingericht volgens de principes van NEN 7513 doordat relevante acties binnen de applicatie en de Azure omgeving worden gelogd, waaronder op dit moment alleen aan en afmeldpogingen, omdat beheerdersomgevingen nog niet bestaan. Deze logs worden voor een vooraf bepaalde termijn bewaard in een niet-muteerbare alleen-toevoegen opslag, zijn uitsluitend toegankelijk voor geautoriseerde beheerders en worden gebruikt voor monitoring, incidentdetectie en forensisch onderzoek.

Tijdens de pilot worden uitsluitend door Glanos geanonimiseerde of gestript verwerkte gegevens verwerkt binnen Azure OpenAI. De onderliggende datacenters van de hostingpartijen zijn ISO 27001 gecertificeerd. Binnen Azure OpenAI wordt een beleid van nulretentie toegepast waarbij gegevens alleen tijdelijk worden gebruikt om output te genereren en daarna automatisch worden verwijderd.

Het Verbond B.V. slaat zelf geen ruwe of herleidbare persoonsgegevens op binnen Doodler.

De Gebruiker heeft het recht om in redelijkheid controle te laten uitvoeren door een onafhankelijke partij, waarbij Het Verbond B.V. medewerking verleent.

5. Incidenten en datalekken

Eventuele incidenten of beveiligingsinbreuken binnen de systemen van Glanos of Microsoft Azure worden conform hun meldplichten aan Het Verbond B.V. gerapporteerd. Doodler meldt deze onverwijld (uiterlijk binnen 24 uur na kennisname) door aan de Gebruiker, inclusief beschrijving van oorzaak, impact en herstelmaatregelen.

Doodler zorgt daarnaast voor de noodzakelijke interne logging op applicatieniveau om beveiligingsincidenten te kunnen detecteren en gepaste herstelmaatregelen te treffen. Deze logging bevat geen cliëntdata of herleidbare informatie en wordt uitsluitend gebruikt voor incidentanalyse en systeembeveiliging.

Het Verbond B.V. verleent volledige medewerking aan onderzoeken en ondersteunt de Gebruiker bij meldingen aan de Autoriteit Persoonsgegevens en/of betrokkenen volgens artikelen 33 en 34 AVG.

6. Leveringszekerheid en aansprakelijkheid

Doodler bevindt zich in een pilot en validatiefase. Tijdelijke onderbrekingen zijn mogelijk.

Het Verbond B.V. spant zich in om beschikbaarheid te waarborgen, maar garandeert geen ononderbroken werking.

Aansprakelijkheid van Het Verbond B.V. is beperkt tot directe schade met een maximum van vijftigduizend euro per incident en honderdduizend euro per jaar, tenzij sprake is van opzet of grove nalatigheid.

Het Verbond B.V. is niet aansprakelijk voor schade die uitsluitend het gevolg is van resterende persoonsgegevens na pseudonimisering, mits aantoonbaar is voldaan aan de overeengekomen beveiligingsmaatregelen en verwerkingen uitsluitend hebben plaatsgevonden binnen de beveiligde omgevingen van de subverwerkers en de eigen Azure omgeving.

6a. Continuïteit en escrow

- Voor de fase na de pilot voorziet Het Verbond B.V. in een escrowregeling bij een erkende partij (zoals Escrow4All), zodat broncode, documentatie en configuraties veilig overdraagbaar zijn.
- In geval van bedrijfsbeëindiging of uitval stelt Het Verbond B.V. instellingen in staat de continuïteit van de dienstverlening te waarborgen. De voortzetting binnen de

eigen Azure-tenant kan plaatsvinden op basis van redelijke commerciële voorwaarden en met ondersteuning door derden.

- Het Continuïteitsplan – beschikbaar als afzonderlijke bijlage – beschrijft de organisatorische en technische maatregelen voor herstel en exit.
-

7. Intellectuele eigendom

Alle rechten op software, algoritmen en methodieken van Doodler berusten bij Het Verbond B.V.

Gebruiker behoudt alle rechten op eigen data en heeft het recht de gegenereerde visualisaties te gebruiken en te archiveren in het cliëntdossier.

8. Toepasselijk recht en geschillen

Op deze voorwaarden is uitsluitend **Nederlands recht** van toepassing.

Geschillen worden in eerste instantie voorgelegd aan de bevoegde rechter te **Utrecht**, tenzij dwingend recht anders bepaalt.

9. Verklaringen

Het Verbond B.V. verklaart dat:

- zij geen toegang heeft tot ruwe of herleidbare cliëntdata;
- de subverwerkers Glanos en Microsoft onder Europees recht vallen en gebruikmaken van datacenters die ISO 27001 gecertificeerd zijn
- Glanos beschikt over een ISAE 3402 type 2 assurance rapport voor informatiebeveiliging
- binnen de pilot uitsluitend gepseudonimiseerde data wordt verwerkt met een beleid van nulretentie in Azure OpenAI
- geen enkele data door Doodler of subverwerkers wordt gebruikt voor training van AI modellen of andere doeleinden dan het genereren van de gevraagde output
- de verwerking uitsluitend plaatsvindt onder opdracht en verantwoordelijkheid van de Gebruiker.

